

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS**

---

IN RE: DEALER MANAGEMENT SYSTEMS  
ANTITRUST LITIGATION

MDL No. 2817  
Case No. 18 C 864

This filing relates to *Authenticom v.  
CDK Global, LLC, et al.*, 18-cv-868

---

**THE REYNOLDS & REYNOLDS COMPANY'S RESPONSE  
IN OPPOSITION TO AUTHENTICOM'S  
MOTION TO DISMISS ONE OF ELEVEN COUNTERCLAIMS (Dkt. 277)**

---

Of the 11 causes of action that Reynolds brought against Authenticom, Authenticom seeks to dismiss only one: conversion. Authenticom has therefore effectively conceded the legal adequacy of Reynolds's claims that Authenticom's business practices are tortious and constitute civil violations of criminal statutes. *See generally* The Reynolds & Reynolds Company's Counterclaims (Dkt. 225). More specifically, Authenticom has not challenged that:

- Each time Authenticom accesses the Reynolds DMS without Reynolds's authorization, it violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), *see* Countercl., Dkt. 225, Count 1 ¶¶ 102-112; the Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a), *see id.*, Count 4 ¶¶ 136-141; and the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502(c)-(e), *see id.*, Count 5 ¶¶ 142-148;
- Each time Authenticom runs the DMS PC software program on a dealer PC; "screen scrapes" original screen layouts, graphical content, and text; or runs pirated copies of the DMS PC software on its own computer systems, it infringes Reynolds's registered copyrights in the Reynolds DMS PC software, *see id.*, Count 2 ¶¶ 113-123;
- Each time Authenticom circumvents Reynolds's DMS access controls (including passwords, CAPTCHA controls, and Suspicious User ID monitoring), and every time it sells its data extraction services for the Reynolds DMS, it violates the Digital Millennium Copyright Act, 17 U.S.C. § 1201, *see id.*, Count 3 ¶¶ 124-135;
- Each time Authenticom induces dealers to provide it with login credentials and DMS system access in knowing contravention of Reynolds's DMS license restrictions, it tortiously interferes with Reynolds's contractual relationships with those dealers, *see id.*, Count 6 ¶¶ 149-156;
- Each time Authenticom's automated scripts execute high-volume transactions on the

Reynolds DMS, thereby impairing DMS system performance and stability by taxing Reynolds's DMS servers, it commits a trespass to chattels with regard to those servers, *see id.*, Count 7 ¶¶ 157-161;

- Every penny of profit that Authenticom has made through its Reynolds DMS data extraction business constitutes unjust enrichment, entitling Reynolds to restitution and disgorgement of those profits or payment of a retroactive licensing fee, *see id.*, Count 9 ¶¶ 167-172;
- Authenticom's unfair and unlawful business practices constitute a violation of the California Unfair Competition Law, entitling Reynolds to an injunction and restitution, *see id.*, Count 10. ¶¶ 173-179;
- Each time Authenticom logs onto, accesses, and uses the Reynolds DMS, it fraudulently misrepresents that it is a bona fide human dealership employee that is authorized to access the Reynolds DMS, *see id.*, Count 11 ¶¶ 180-187.

Further, Authenticom's Motion fails in its central task: Reynolds's claim for conversion is incontrovertibly adequately pleaded. Authenticom's Motion should be denied.

#### **I. Authenticom's Suit is a Classic Effort to Recast its Own Illegal Conduct**

Authenticom's antitrust claims cannot disguise the fact that its Reynolds-oriented "data integration" services are wholly illegal. As Reynolds made clear for years before any alleged agreement with CDK, Reynolds unilaterally prohibits Authenticom's hostile and unauthorized access to its system. Authenticom is not privileged to hijack credentials, scrape processed data, and resell it. Authenticom's efforts to evade Reynolds's unilateral measures are illegal, and its attempt to recast this illegal activity must fail.

Indeed, long before Authenticom came up with its amorphous antitrust claims against Reynolds and CDK, Reynolds sent Authenticom a cease-and-desist letter formally notifying Authenticom that its unauthorized access to the Reynolds DMS constituted, at the very least, tortious interference with Reynolds's DMS license contracts with its dealers. *See id.* ¶¶ 68-69. Authenticom disregarded that notice and continued its program of obtaining Reynolds DMS user IDs, hacking into the Reynolds DMS, and slamming DMS servers with automated data

transactions that impaired system stability and performance. Although Reynolds deferred filing suit against Authenticom while continuing to focus on cybersecurity measures, Reynolds is (and always has been) the true plaintiff here. Reynolds's longstanding system measures are valid unilateral conduct, and Authenticom's antitrust claims are simply an effort to accomplish via legal process what it could not via continued hacking.<sup>1</sup> Authenticom's actions in contravention of Reynolds's intellectual property rights are illegal independent of any of Authenticom's manufactured claims. Reynolds is entitled to an injunction against Authenticom's unauthorized access to its system as well as damages.

## **II. Authenticom's Suggestion that the Dealers' Authorization Excuses Its Conduct is False**

The outset of Authenticom's Motion asserts that "the *dealerships'* authorization is all the authorization Authenticom needs," and therefore "Reynolds' claims are . . . untenable," but Authenticom has no support for those assertions. Authenticom, Inc.'s Memorandum in Support of Its Partial Motion to Dismiss the Counterclaims of the Reynolds & Reynolds Company (the "Motion"), Dkt. 278 at 1-2. As Authenticom has known for years, such authorization-by-proxy is impossible. The dealerships did not pay to develop the system, have no authority to grant access to it, and agreed by contract not to give access to non-employee users as part of their negotiated license. No doubt Authenticom wants to defer any ruling on the Computer Fraud and Abuse Act (the "CFAA") until as late as possible in this litigation. Authenticom knows that any decision on

---

<sup>1</sup> Authenticom's separate motions to dismiss filed against Reynolds and CDK highlight the distinct and unilateral nature of Reynolds's longstanding prohibition on hostile access to its system and underscore the invalidity of Authenticom's own claims of some "conspiracy." In its Reynolds-directed motion, Authenticom does not and cannot point to any change in Reynolds's longstanding unilateral prohibition on access to its system by parties like Authenticom in its contracts or otherwise. *See generally*, Motion, Dkt. 278. As Judge St. Eve already found, summarizing the black letter law in *Trinko* and the Seventh Circuit's prior decision in this case, Authenticom's attempts to garner forced sharing of Reynolds's DMS runs "afoul of the bedrock principle that firms generally have no duty to deal with competitors." Order, Dkt. 176 at 2, *citing Authenticom, Inc. v. CDK Glob., LLC*, 874 F.3d 1019, 1021 (7th Cir. 2017) and *Verizon Commc'ns Inc. v. Law Offices of Curtis v. Trinko*, 540 U.S. 398 (2004).

the CFAA will be an effective kill shot<sup>2</sup> to its antitrust claims, because Authenticom’s position—that a dealer can unilaterally excuse Authenticom’s hacking into *Reynolds*’s computer systems—is flatly contradicted by the language of the statute and the holdings of the leading cases construing the statute on similar facts. See Brief of Defendant-Appellant The Reynolds and Reynolds Company at 31-37, Dkt. 47, *Authenticom, Inc. v. CDK Global, LLC, et al.*, 874 F.3d 1019 (7<sup>th</sup> Cir. 2017) (No. 17-2541); Reply Brief of Defendant-Appellant The Reynolds and Reynolds Company at 11-15, Dkt. 70, *Authenticom, Inc. v. CDK Global, LLC, et al.*, 874 F.3d 1019 (7<sup>th</sup> Cir. 2017) (No. 17-2541); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9<sup>th</sup> Cir. 2016), *cert. denied*, 138 S. Ct. 313, 199 L. Ed. 2d 206 (2017).<sup>3</sup>

Authenticom *affirmatively pleads* that Reynolds has unilaterally imposed and enforced its prohibition on third-party access since at least 2009, nearly a decade ago. See Authenticom’s Complaint, No. 1:18-cv-00868, Dkt. 1, at ¶ 189 (“Reynolds first started disabling Authenticom’s

---

<sup>2</sup> In addition, Dealers cannot grant Authenticom permission to infringe Reynolds’s copyrights, circumvent Reynolds’s DMS system access controls, or carry out myriad violations of Reynolds’s common-law rights. As Authenticom concedes, the Reynolds DMS license prohibits dealers from allowing third-party access to the DMS, and Authenticom chose not to replead its tying and exclusive dealing claims attacking that contractual prohibition after Judge St. Eve dismissed them. Those contract restrictions are *independent* of any alleged antitrust claims are, thus, an *independent* bar to antitrust injury regardless of this Court’s resolution of the issues in *Authenticom*’s live complaint. See Reynolds’s Memorandum in Support of Motion to Dismiss the Dealership Class Action, Dkt. 255, at 47-48.

Judge St. Eve’s ruling that “Authenticom’s as-alleged practices are not illegal independent of Defendants’ challenged conduct,” because “the question of this case is whether Defendants’ refusal to grant such authorization and access . . . was the result not of a unilateral refusal to deal, but of illegal conspiracies and anticompetitive arrangements (like tying or exclusive dealing) recognized by the antitrust laws” is no longer pertinent. Dkt. 176 at 20-21 & 21 n.7. Judge St. Eve *dismissed* the tying and exclusive dealing allegations targeted at the provisions of the DMS license prohibiting third-party access, and Authenticom did not attempt to replead them. The restrictions in the dealer licenses against hostile access are not at issue, are valid, and mean, in short, that *independent* of any alleged conduct by Reynolds, Authenticom’s access is illegal.

<sup>3</sup> Judge Easterbrook’s bruising treatment of Authenticom’s position on the CFAA at the Seventh Circuit oral argument is a strong indicator that the Seventh Circuit will follow the Ninth and myriad other courts in flatly rejecting Authenticom’s suggestion that a computer-system *user* can grant permission effective to obviate a CFAA claim when the computer-system *owner* withholds permission. As Judge Easterbrook explained, “Authenticom wants to get information from protected computers within the meaning of [the CFAA] . . . But [authorization] is not being granted by the person who runs the system. That is, by CDK or Reynolds.” “[T]o get access to AOL’s system you need AOL’s permission, not my permission. The fact that I have an account with AOL doesn’t mean I can authorize anyone else to use AOL.” Dkt. 255, Ex. 7 (Seventh Circ. Trans.) at 50:19-55:2.

usernames in 2009 when it introduced... ‘challenge questions’ and ‘captcha’”). And Authenticom pleads no facts to suggest that Reynolds was on the verge of changing that policy when the 2015 agreement with CDK was entered. Authenticom does not dispute that Reynolds has prohibited third-party DMS access for over a decade; has never considered permitting third-party access; and has never had any reason to consider permitting third-party access. The proof is in the pudding. In its Motion, Authenticom does not dispute that Reynolds has pled a valid claim against Authenticom for Authenticom’s illegal hacking of Reynolds’s system.

### **III. Reynolds’s Conversion Claim is Adequately Pleaded**

Authenticom’s cursory argument for dismissal of Reynolds’s conversion claim fails. “A person is liable for conversion when he or she (1) intentionally controls or takes property belonging to another, (2) without the owner’s consent, (3) resulting in serious interference with the owner’s rights to possess the property.” *Midwestern Helicopter, LLC v. Coolbaugh*, 2013 WI App 126, ¶ 9, 351 Wis. 2d 211, 217, 839 N.W.2d 167, 170 (citing *H.A. Friend & Co. v. Prof’l Stationery, Inc.*, 2006 WI App 141, ¶ 11, 294 Wis. 2d 754, 763, 720 N.W.2d 96, 100). Authenticom’s only argument is that Reynolds has not alleged facts sufficient to satisfy the third element, “serious interference with the owner’s rights to possess the property,” but Authenticom’s Motion ignores the detailed allegations in the Counterclaims regarding Authenticom’s serious interference.<sup>4</sup>

“[W]hether an unauthorized exercise of dominion constitutes conversion depends on the severity of interference with the owner’s right to control.” *Midwestern Helicopter*, 839 N.W.2d at

---

<sup>4</sup> Reynolds also satisfies the pleading standard for the first two elements. Paragraph 163 of the Counterclaims states that: “Every time Authenticom accessed and ran the Reynolds DMS PC software program, it intentionally controlled Reynolds-owned servers, which are located at the dealer sites or at Reynolds’s server farms. Use of the DMS PC software program sends instructions to the Reynolds-owned server systems, which execute the instructions and send back a response.” Dkt. 225, ¶ 163. That satisfies the control element: Authenticom caused Reynolds’s server systems to execute computing instructions. And the Counterclaims are replete with detailed allegations demonstrating Reynolds’s lack of consent to Authenticom’s use of its computer systems. *See, e.g.*, Dkt. 225 ¶¶ 32, 50-66, 68, 71-78.

220 (citing Restatement (Second) of Torts § 222A (1965)).<sup>5</sup> Authenticom agrees that Restatement Section 222A furnishes the relevant standard. See Mot., Dkt. 278 at 4 (citing Section 222A three times). But Authenticom ignores Section 222A’s detailed standard for evaluating the “serious interference” element and compounds the error by ignoring the many factual allegations in the Counterclaims that easily satisfy that standard.<sup>6</sup> Section 222A provides:

In determining the seriousness of the interference and the justice of requiring the actor to pay the full value, the following factors are important:

- (a) the extent and duration of the actor’s exercise of dominion or control;
- (b) the actor’s intent to assert a right in fact inconsistent with the other’s right of control;
- (c) the actor’s good faith;
- (d) the extent and duration of the resulting interference with the other’s right of control;
- (e) the harm done to the chattel;
- (f) the inconvenience and expense caused to the other.

Authenticom’s Motion is a strawman: Reynolds has pleaded detailed allegations that support each of these factors.

Authenticom has executed computing instructions on the DMS servers hundreds or thousands of times per day, thereby impairing system performance and crowding out legitimate

---

<sup>5</sup> Wisconsin courts—just like Authenticom in its Motion—rely heavily on the Restatement (Second) of Torts. See, e.g., *Brandenburg v. Briarwood Forestry Services, LLC*, 2014 WI 37, 354 Wis. 2d 413, 847 N.W.2d 395 (extensively citing and analyzing Restatement (Second) of Torts); *Hocking v. City of Dodgeville*, 2009 WI 70, 318 Wis. 2d 681, 768 N.W.2d 552 (same); *Vogel v. Grant-Lafayette Elec. Co-op.*, 201 Wis. 2d 416, 423, 548 N.W.2d 829, 832–33 (1996) (same); *Baumeister v. Automated Products, Inc.*, 2012 WI App 27, 339 Wis. 2d 489, 809 N.W.2d 900 (same); *Hanley Implement Co., Inc. v. Riesterer Equip., Inc.*, 150 Wis. 2d 161, 166, 441 N.W.2d 304, 305 (Ct. App. 1989) (citing Restatement for conversion claim).

<sup>6</sup> In evaluating a Rule 12(b)(6) motion to dismiss, the Court evaluates the complaint as a whole, not individual allegations or counts taken in isolation. E.g., *Engel v. Buchan*, 710 F.3d 698, 710 (7th Cir. 2013) (evaluating allegations “sensibly and as a whole”). Thus, if Reynolds’s Counterclaims *as a whole* pleads facts sufficient to establish a claim for conversion, this Court should deny Authenticom’s Motion.

transactions, over a span of years—satisfying factors (a) [extent and duration of control] and (d) [extent and duration of interference]. Countercl., Dkt. 225 ¶¶ 99, 165. It has done so with explicit intent to deny Reynolds’s exclusive right to control the servers, boasting that it would continue to hack into and use the DMS (control) “despite whatever hurdles” Reynolds placed in its path, satisfying factor (b) [intent to assert right inconsistent with Reynolds’s right of control]. *Id.* ¶ 80. Indeed, Authenticom’s affirmative claims are fundamentally predicated on the misguided notion that Reynolds has no right to control its own DMS servers and must instead open its computer systems to use by all comers. Authenticom has also at all relevant times known that its use of the Reynolds system and hacked control of the servers was unauthorized, and has thereby acted in bad faith by doubling down on its efforts to use and control Reynolds’s DMS servers for its own gain despite this knowledge, satisfying factor (c) [bad faith]. *E.g., id.* ¶ 152.

Finally, the allegations easily satisfy factors (e) [harm] and (f) [inconvenience and expense]. Authenticom’s daily, high-volume commandeering of Reynolds’s DMS servers “taxes the computational and network resources of the Reynolds DMS, resulting in degradation of service for dealers and increased operational costs to Reynolds.” *Id.* ¶ 99. “It has been expensive and burdensome for Reynolds to respond to Authenticom’s continuing technological gamesmanship and ‘Whack-A-Mole’ tactics. Reynolds has had to invest significant resources in investigating and resolving hostile integration problems caused by Authenticom . . . .” *Id.* ¶ 101. Further, Authenticom’s high-volume usage crowds out legitimate transactions on the DMS servers. *Id.* ¶ 165. Reynolds’s detailed factual allegations easily satisfy the “serious interference” element of its conversion claim.

Additional support comes from Restatement Section 227, “Conversion by Using Chattel.” That Section states the simple rule that “[o]ne who uses a chattel in a manner which is a serious



violation of the right of another to control its use is subject to liability to the other for conversion.” The comments and illustrations that follow are instructive. First, Comment B emphasizes that a proper analysis takes into account the Section 222A factors discussed above (but ignored by Authenticom). Second, it stakes out the spectrum of potential fact patterns in conversion-through-use cases: “A single, temporary, and unimportant use which does not damage the chattel or inconvenience the owner, and is not intended as a defiance of his rights, may not be enough for a conversion, whereas an extended use, one which causes damage, or one intended as the assertion of an adverse claim may be sufficient.” Restatement (Second) of Torts § 227, cmt. b. Authenticom’s conduct satisfies all three of the *disjunctively* stated categories in the latter half of that sentence. Finally, the Illustrations make the point plain:

1. A owns a desk, which is his private property. On one occasion, without A’s consent, B uses the desk to write his wife. This is not a conversion of the desk.
2. The same facts as in Illustration 1, except that B uses the desk daily for six months. This is a conversion.

Under the logic of Illustration 2, Authenticom—who has commandeered the DMS servers hundreds or thousands of times, every day, for years—has committed a conversion of those assets.

The two cases that Authenticom cites for the proposition that “courts have rejected the attempt to equate unauthorized access with conversion” are easily distinguishable. If anything, *DIRECTV, Inc. v. Massey*, 03 C 3492, 2004 WL 1194744, at \*4 (N.D. Ill. May 27, 2004) *supports* Reynolds’s position. First, it is not a case about unauthorized use of a computer system. Instead, the defendant allegedly purchased and used a device that received and unscrambled DIRECTV’s broadcasted satellite TV signals. Second, as with the Restatement, the context of Authenticom’s pull-quote demonstrates the weakness of its argument. Authenticom accurately quotes the opinion’s statement that “there are no allegations that [Defendants] exercised such dominion and control over the signals as to deprive DIRECTV, the rightful owner of the signals, the use of them.”



Mot., Dkt. 278 at 5 (quoting *DIRECTV*, 2004 WL 1194744, at \*4). But the first half of that quoted sentence is: “The satellite signals are broadcast into the open air . . . .” *DIRECTV*, 2004 WL 1194744, at \*4. And the next sentence is: “DIRECTV has not alleged that any of the signals sent to its paying customers were disrupted as a result of [Defendant’s] interception or that DIRECTV was somehow unable to enjoy the benefit of those signals sent out.” *Id.* By contrast, the Reynolds DMS servers are *not* nonrival goods broadcasted in waveform that Authenticom happened to descramble after picking them up on an antenna. Instead, they are specific physical objects with limited processing capacity whose functionality and performance are routinely degraded by Authenticom’s day-in, day-out commandeering, thus interfering with legitimate use of the servers. *E.g.*, Countercl., Dkt. 225 ¶¶ 99, 101, 165. The strong implication of the *DIRECTV* decision is that, if similar allegations had been present, the conversion claim would have survived.

Authenticom’s citation to *Scs Healthcare Marketing, LLC v Allergan Usa, Inc.*, No. C-268-12, 2012 WL 6565713 (N.J. Super. Ch., Bergen County Dec. 07, 2012) is similarly inapposite, and its parenthetical description of the case’s holding is misleading. Authenticom parenthetically describes the case as “(granting motion to dismiss conversion claim and noting that in the ‘context of unauthorized computer access’ claims, courts have ‘been reluctant to find conversion where there is no tangible [personal] property taken.’)” Mot., Dkt. 278 at 5. But *Scs Healthcare* did not involve a claim for conversion of a computer system through unauthorized use, nor was the conversion claim dismissed for the reason suggested by Authenticom’s quote. The *Scs Healthcare* plaintiff alleged that the defendant had converted *trade secrets*, not a computer system, after accessing a computer system nine times and exfiltrating trade secret information from it. *Scs Healthcare*, 2012 WL 6565713, Slip Op. 2, 10.<sup>7</sup> The conversion claim was dismissed exclusively

---

<sup>7</sup> Westlaw’s text version of the case is unpaginated, but the slip opinion is available as an original image. The page citations in this brief are to the slip opinion pages.

because, under New Jersey law, one cannot convert intangible trade secrets. *Id.* at 10. The court did not consider or dismiss any allegation that *accessing* the computer nine times constituted conversion of that computer. The plaintiff separately alleged that the defendant had committed a trespass to chattels by accessing the computer system. *Id.* at 10. The material that Authenticom excerpts is from the court’s discussion of the trespass to chattels claim, not the conversion claim. Moreover, it is not even a quotation of the court’s own words. Instead, it is simply secondary authority from a local, New Jersey business litigation treatise that is entirely inconsistent with the applicable Wisconsin law. Under the rules set out in both Wisconsin caselaw and the Restatement, the instant case is entirely dissimilar to the “unauthorized access” cases described in that treatise excerpt. The New Jersey secondary authority cited by Plaintiffs opines that “unauthorized access to a computer does not deprive the owner of the value and/or use of the computer, as is typically required to sustain an action in conversion.” *Id.* But of course, Reynolds pleads exactly that. This is not a normal case of one-off computer trespass: it is a case of routine computer commandeering. Likewise, Plaintiffs’ New Jersey treatise states: “[c]ourts have been reluctant to find conversion where there is no tangible property taken.” *Id.* But here, Reynolds alleges precisely that Authenticom’s remote commandeering of its servers has deprived it of the use and value of its tangible property. And under applicable Wisconsin law, “taking” is not a necessary element—“controlling” another’s property in a manner that seriously interferes with possessory rights is sufficient. *Midwestern Helicopter*, 839 N.W.2d at 167. Reynolds has unquestionably pled a sufficient claim of conversion.

#### **IV. Conclusion**

Reynolds’s conversion claim is legally adequate, and so this Court should deny Authenticom’s Motion. Moreover, Reynolds respectfully submits that there is no basis to extend

Authenticom's time to answer beyond the 14 days from the date of the court's decision set out in Rule 12(a)(4). By the time Authenticom files its Reply, it will have had roughly ten weeks during which it could have drafted an Answer. And given that Authenticom moved to dismiss only one of Reynolds's eleven claims, there is no meaningful uncertainty as to what portions of the Counterclaims it will need to answer. The only allegations that are exclusively relevant to the conversion claim are the five paragraphs of the count itself; all of the other factual allegations in the Counterclaims are either primarily or additionally relevant to one or more other claims that Authenticom has not moved to dismiss and that it will need to answer regardless of the outcome of this Motion. Thus, extending Authenticom's deadline to answer even more than has already occurred by operation of law on filing of its Motion is unwarranted.

Dated: August 20, 2018

Respectfully submitted,

/s/ Aundrea K. Gulley

Aundrea K. Gulley

agulley@gibbsbruns.com

Kathy Patrick

kpatrick@gibbsbruns.com

Brian T. Ross

bross@gibbsbruns.com

Brice A. Wilkinson

bwilkinson@gibbsbruns.com

Ross M. MacDonald

rmacdonald@gibbsbruns.com

Justin D. Patrick

jpatrick@gibbsbruns.com

**GIBBS & BRUNS, LLP**

1100 Louisiana, Suite 5300

Houston, Texas 77002

Telephone: 713-650-8805

Facsimile: 713-750-0903

Michael P.A. Cohen

MCohen@sheppardmullin.com

Amar S. Naik

ANaik@sheppardmullin.com  
**SHEPPARD MULLIN RICHTER  
& HAMPTON LLP**  
Suite 100  
2099 Pennsylvania Avenue, N.W.  
Washington, D.C. 20006  
Telephone: 202-747-1900  
Facsimile: 202-747-1901

Leo D. Caseria  
**SHEPPARD MULLIN RICHTER  
& HAMPTON, LLP**  
333 S. Hope St., 43rd Floor  
Los Angeles, CA 90071  
(213) 617-4206  
lcaseria@sheppardmullin.com

Dylan I. Ballard  
**SHEPPARD MULLIN RICHTER  
& HAMPTON, LLP**  
Four Embarcadero Center., 17th  
Floor  
San Francisco, CA 94111  
(415) 434-9100  
dballard@sheppardmullin.com

*Attorneys for Defendant and Counterplaintiff  
The Reynolds and Reynolds Company*

**CERTIFICATE OF SERVICE**

I, Aundrea K. Gulley, an attorney, hereby certify that on this 20th day of August, 2018, I caused a true and correct copy of the foregoing Response in Opposition to Authenticom's Motion to Dismiss One of Eleven Counterclaims to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF system.

/s/ Aundrea K. Gulley

Aundrea K. Gulley

**GIBBS & BRUNS LLP**

1100 Louisiana Street, Suite 5300

Houston, TX 77002

(713) 650-8805

agulley@gibbsbruns.com